Data Sheet

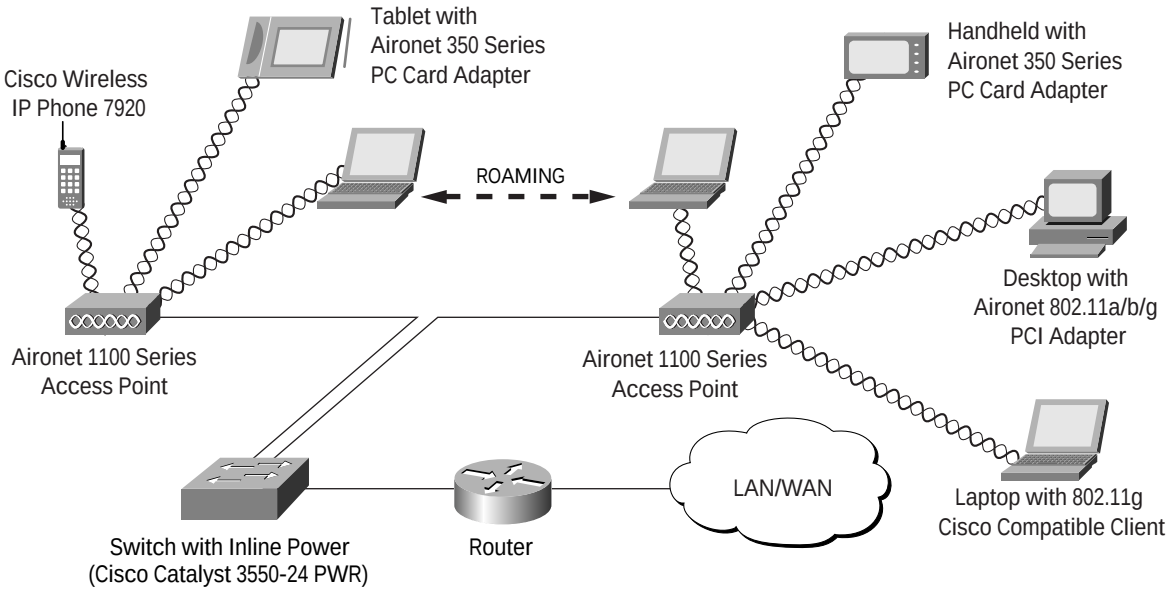
Cisco Aironet 1100 Series Access Point

The Cisco Aironet® 1100 Series Access Point provides a high-speed, secure, affordable, and easy-to-use wireless LAN solution that combines the freedom and flexibility of wireless networking with the features and services required in enterprise networks (Figure 1). The Cisco Aironet 1100 Series supports a single radio and is available in an IEEE 802.11g version or IEEE 802.11b version. The IEEE 802.11b version is field upgradable to 802.11g.

The access point offers flexibility and investment protection for wireless networks. With the IEEE 802.11g version, users can enjoy up to 54 Mbps data rates while maintaining full backward compatibility with legacy 802.11b devices. Administrators can configure the access point to support both 802.11g and legacy 802.11b clients for investment protection or, for higher performance, it may be configured to support only 802.11g clients. The Cisco Wireless Security Suite provides the strongest enterprise security solution available while the Cisco IOS® Software operating system delivers enterprise-class services with a familiar user interface. The Cisco Aironet 1100 Series also features integrated diversity dipole antennas and an innovative mounting system for easy installation and reliable coverage in a variety of locations and orientations.

Figure 1

An access point either is the center point in an all-wireless network or serves as a connection point between a wired and wireless network. Multiple access points can be placed throughout a facility to give users with 802.11b or 802.11g wireless LAN client adapters the ability to roam freely throughout an extended area while maintaining uninterrupted access to all network resources.



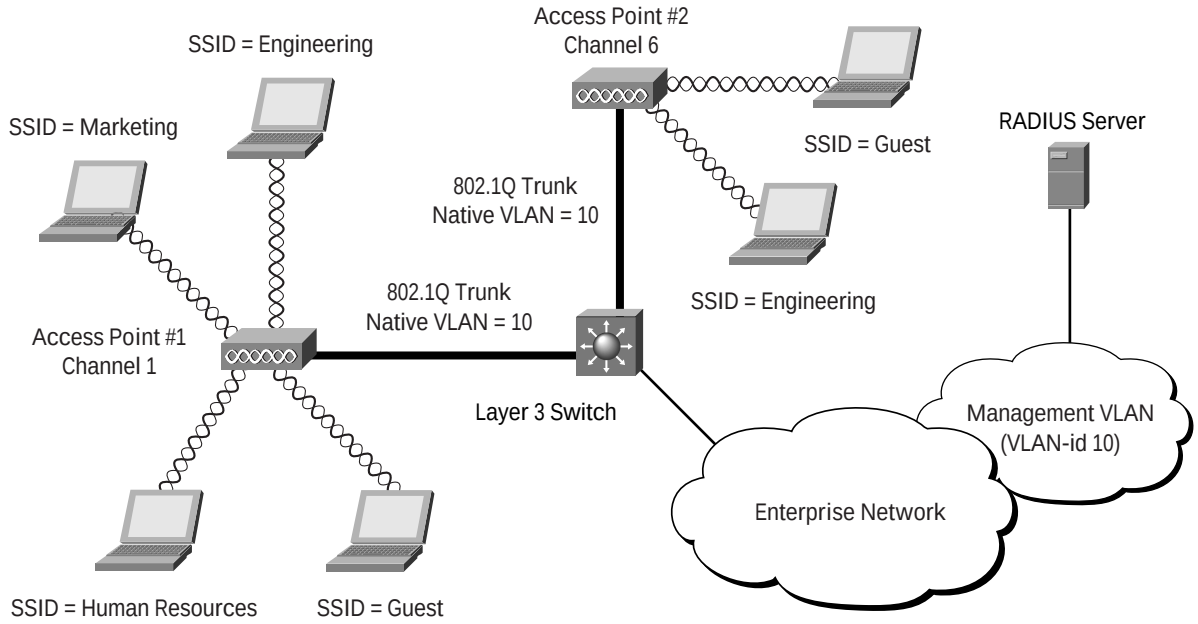
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Intelligent Networking Features for a Scalable, Manageable Solution

The Cisco Aironet 1100 Series extends end-to-end intelligent networking to the wireless access point. Cisco command-line interface (CLI) allows customers to quickly and consistently implement the extended capabilities available in Cisco IOS Software. Customers can manage and standardize their networks using tools they have developed internally for their Cisco routers and switches.

An ideal choice for enterprise installations, the Cisco Aironet 1100 Series supports enterprise-class virtual LANs (VLANs), quality of service (QoS) and proxy mobile IP. The Cisco Aironet 1100 Series can manage up to 16 VLANs (Figure 2), which allows customers to differentiate LAN policies and services, such as security and QoS, for different users. For example, enterprise customers can use different VLANs to segregate employee traffic from guest traffic, and further segregate those traffic groups from high-priority voice traffic. Traffic to and from wireless clients with varying security capabilities can be segregated into VLANs with varying security policies. Another example would be educational institutions that use VLANs to secure faculty and administrator traffic from student traffic traveling over the same infrastructure. Implementing VLAN segmentation increases wireless LAN manageability and security.

Figure 2
Indoor Wireless VLAN Deployment



With support for 802.1p QoS, the Cisco Aironet 1100 Series provides traffic prioritization for packets traveling to and from the access point over Ethernet. Delay-sensitive traffic, such as voice and video, can be prioritized over data traffic for improved user experience and optimal network utilization. Software and radio firmware upgrades allow upgrades to future QoS standards such as 802.11e. Supporting the voice prioritization schemes for 802.11b mobile phones, the Aironet 1100 Series further enables quality voice-over-wireless-LAN solutions.

With proxy mobile IP, users can maintain seamless network connectivity as they roam across subnets. The proxy mobile IP feature creates a tunnel between routers on the remote network and the user's home network. This allows users to consistently maintain their home IP address and access to their home network applications as they roam beyond their home subnet. Proxy mobile IP also enhances a mobile IP-enabled network by enabling subnet roaming

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

capabilities on IEEE 802.11 clients so that these devices do not need specialized mobile IP client software, resulting in additional cost-savings. These proxy mobile IP features enable IT professionals to use their existing IP addressing scheme to cost-effectively design the wireless LAN in a manner more consistent with the wired LAN, while still maintaining user mobility.

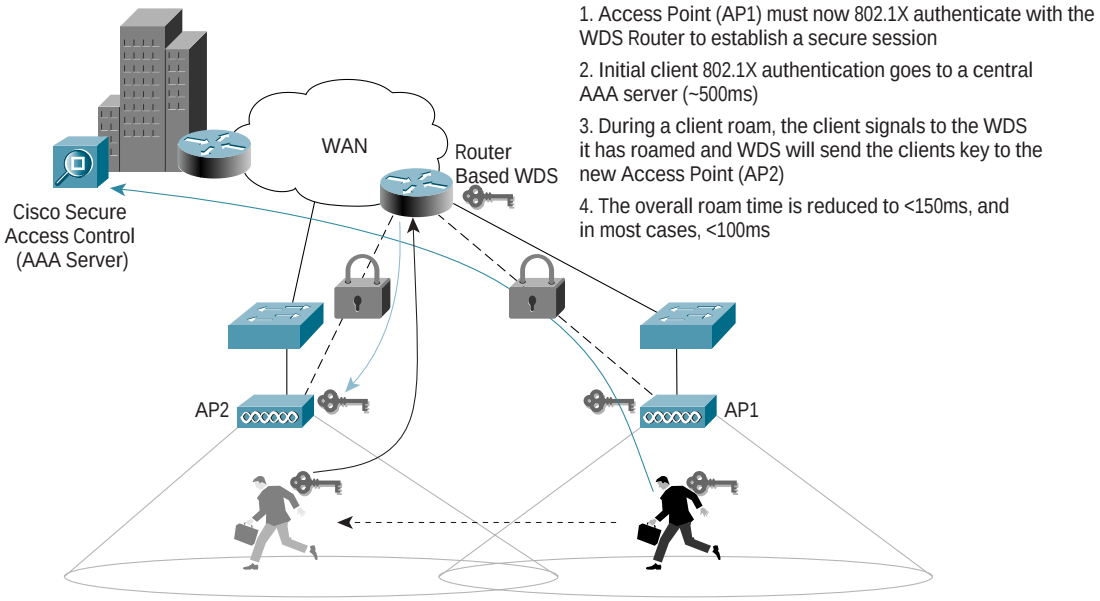
Cisco Structured Wireless-Aware Network

The Cisco Aironet 1100 Series is a key component of the Cisco Structured Wireless-Aware Network (SWAN). Cisco SWAN is an innovative, comprehensive Cisco framework for deploying, operating, and managing hundreds to thousands of Cisco Aironet access points using the Cisco infrastructure. Cisco SWAN extends to the wireless LAN the same level of security, scalability, and reliability that customers have come to expect in their wired LAN by introducing "wireless-aware" capabilities into the Cisco infrastructure.

Wireless domain services (WDS) is introduced with Cisco SWAN. WDS is a collection of Cisco IOS Software features that expand WLAN client mobility, simplify WLAN deployment and management and enhance WLAN security. These services, supported on access points and client devices today and on specific Cisco LAN switches and routers in 2004, include radio management aggregation, fast secure roaming and WAN link remote site survivability. WDS radio management aggregation supports radio frequency (RF) managed services such as rogue access point detection, interference detection and assisted site surveys.

To take advantage of the innovative features of the 1100 Series, not only can Cisco client adapters be used, but now a wide variety of Cisco Compatible devices are available from leading WLAN client suppliers. For example, fast secure roaming is supported by the Cisco Aironet 1100 Series in conjunction with Cisco or Cisco Compatible client devices. With fast secure roaming, authenticated client devices can roam securely from one access point to another without any perceptible delay during reassociation. Fast secure roaming supports latency-sensitive applications such as wireless voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions (Figure 3).

Figure 3
Fast Secure Roaming

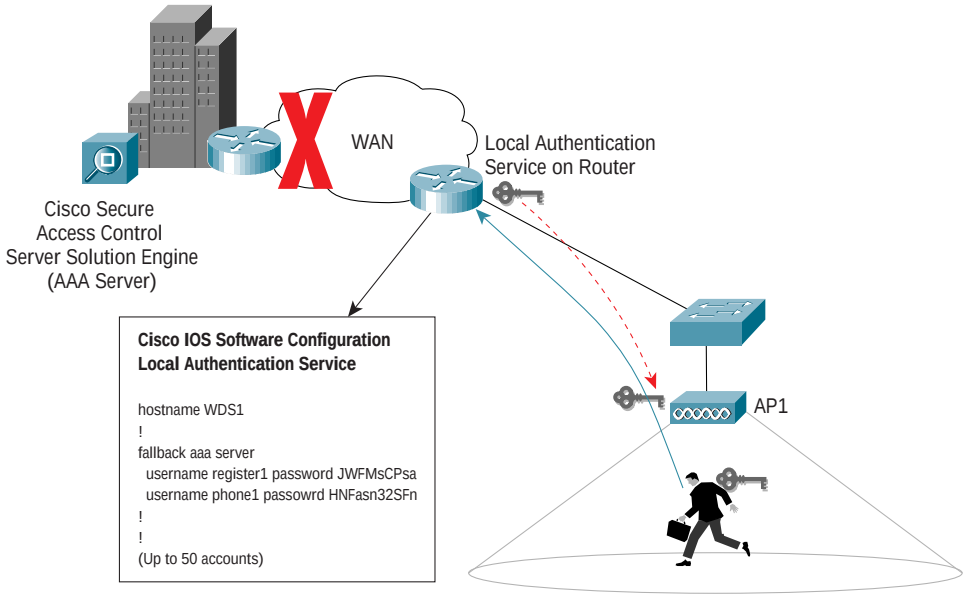

1. Access Point (AP1) must now 802.1X authenticate with the WDS Router to establish a secure session
2. Initial client 802.1X authentication goes to a central AAA server (~500ms)
3. During a client roam, the client signals to the WDS it has roamed and WDS will send the clients key to the new Access Point (AP2)
4. The overall roam time is reduced to <150ms, and in most cases, <100ms
WAN
Router Based WDS
Cisco Secure Access Control (AAA Server)
AP2
AP1

Note: Because the WDS handles roaming and reauthentication, the WAN link is not used

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

WAN link remote site survivability allows the access point to act as a local RADIUS server to IEEE 802.1X authenticate wireless clients when the authentication, authorization, and accounting (AAA) server is not available. This provides remote site survivability and backup authentication services during a WAN link or server failure allowing users in remote site deployments with nonredundant WAN links access to local resources such as file servers or printers (Figure 4).

Figure 4
WAN Link Remote Site Survivability



Enterprise-Class Security Solution

Wireless LAN security is a primary concern. The Cisco Aironet 1100 Series secures the enterprise network with a scalable and manageable system featuring the award-winning Cisco Wireless Security Suite. Based on the 802.1X standard for port-based network access, the Cisco Wireless Security Suite takes advantage of the Extensible Authentication Protocol (EAP) framework for user-based authentication (Figure 5). This solution also supports Wi-Fi Protected Access (WPA), the new Wi-Fi Alliance specification for interoperable, standards-based wireless LAN security.

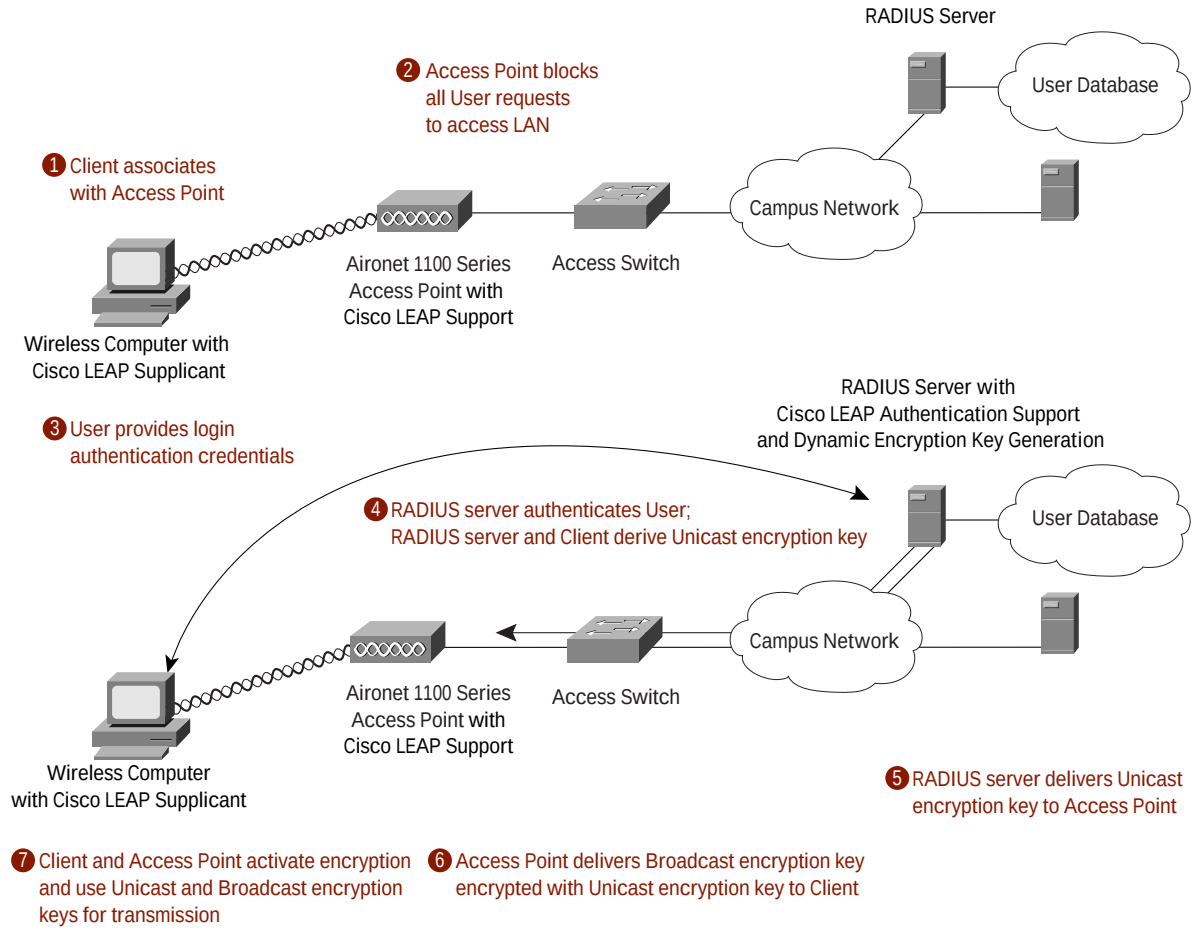
The Cisco Wireless Security Suite interoperates with a range of client devices. It supports all 802.1X authentication types, including Cisco LEAP, Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) and types that operate over EAP-TLS, such as Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled TLS (EAP-TTLS) and EAP-Subscriber Identity Module (EAP-SIM). A wide selection of RADIUS servers, such as the Cisco Secure Access Control Server (ACS), can be used for enterprise-class centralized user management that includes:

- Strong, mutual authentication to ensure that only legitimate clients associate with legitimate and authorized network RADIUS servers via authorized access points
- Dynamic per-user, per-session encryption keys that automatically change on a configurable basis to protect the privacy of transmitted data

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- Stronger encryption keys provided by Temporal Key Integrity Protocol (TKIP) enhancements such as message integrity check (MIC), per-packet keys via initialization vector hashing, and broadcast key rotation
- Ready for Advanced Encryption Standard (AES) support
- RADIUS accounting records for all authentication attempts

Figure 5
The Cisco Wireless Security Suite is an Enterprise-Class Security System Based on the 802.1X Architecture


RADIUS Server
User Database
2 Access Point blocks all User requests to access LAN
1 Client associates with Access Point
Campus Network
Aironet 1100 Series Access Point with Cisco LEAP Support
Access Switch
Wireless Computer with Cisco LEAP Supplicant
RADIUS Server with Cisco LEAP Authentication Support and Dynamic Encryption Key Generation
3 User provides login authentication credentials
4 RADIUS server authenticates User; RADIUS server and Client derive Unicast encryption key
User Database
Campus Network
Aironet 1100 Series Access Point with Cisco LEAP Support
Access Switch
Wireless Computer with Cisco LEAP Supplicant
5 RADIUS server delivers Unicast encryption key to Access Point
7 Client and Access Point activate encryption and use Unicast and Broadcast encryption keys for transmission
6 Access Point delivers Broadcast encryption key encrypted with Unicast encryption key to Client

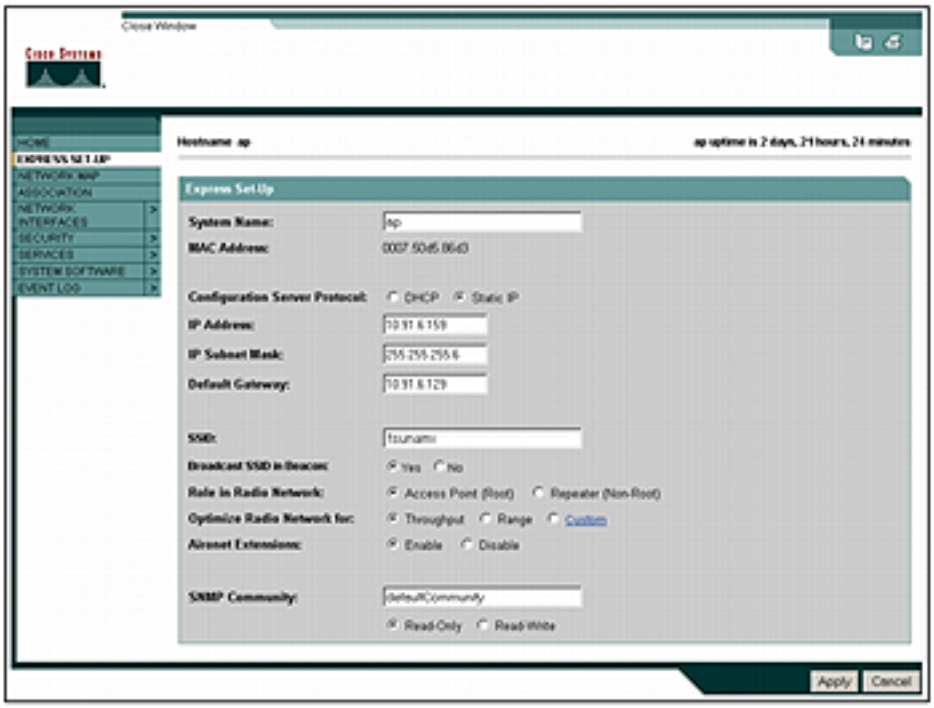
Simplified Deployment for Rapid Connectivity

The Cisco Aironet 1100 Series, with its redesigned graphical user interface (GUI), introduces the next level of intuitive, browser-based management for an improved user experience (Figure 6). A menu-based organization simplifies navigation and configuration for easy setup and ongoing management with uncompromised security. The Cisco Aironet 1100 Series can also be managed using Cisco IOS Software CLI, which is familiar to IT professionals, allowing them to rely on existing skills in both management and deployment.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 6

The redesigned GUI in the Aironet 1100 Series provides intuitive browser-based management for basic configuration of the access point.



The Cisco Aironet 1100 Series defines enterprise office deployment capability. Designed in an attractive, durable plastic enclosure, with integrated diversity dipole antennas, the Cisco Aironet 1100 Series can be quickly deployed with a reliable, omni-directional coverage pattern. Supported in various mounting orientations and locations, it can be easily moved throughout the work area as needs change (Figure 7). A standard, surface-mounting bracket supports installation on office walls and ceilings for elevated placement. UL 2043 certification for the plenum rating requirements set by local fire codes supports installation in environmental air spaces such as areas above suspended ceilings. The design protects against tampering and theft using single- or master-keyed padlocks. The Cisco Aironet 1100 Series can also be brought into the cubicle space with a cubicle wall-mounting bracket or device stand. The device stand positions the access point on any horizontal surface, such as a desktop or shelf. Theft is deterred in these installations using the security slot with standard security cables. Support for either local or inline power over Ethernet further simplifies installation. The Cisco Aironet 1100 Series is Wi-Fi certified to ensure interoperability with other IEEE 802.11g and IEEE 802.11b devices.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 7
The Cisco Aironet 1100 Series Access Point Mounting Brackets Include Ceiling, Wall, Cubicle, and Desktop Options

Advanced Management of Large Scale Wireless LAN Deployments

The CiscoWorks Wireless LAN Solution Engine (WLSE), a component of the Cisco SWAN, is available as a management tool for Cisco Aironet access points and wireless bridges. CiscoWorks WLSE is a turnkey, scalable, and centralized management platform for managing hundreds to thousands of Cisco Aironet access points and wireless bridges. For more information on CiscoWorks WLSE, visit: http://www.cisco.com/go/wlse

Cost-Effective Solution for Evolving Requirements

The Cisco Aironet 1100 Series is ideal for new deployments, or as an addition to existing deployments to support increasing capacity requirements. Engineered with extra system capacity, including memory, storage, and processing power, the Cisco Aironet 1100 Series is designed to support not only today's feature set, but future software releases for expanded functionality and capabilities.

Key Features and Benefits

The Cisco Aironet 1100 Series merges enterprise features, manageability, security, and availability into a scalable, easy-to-deploy, and cost-effective WLAN solution. Tables 1-3 highlight key features, product specifications, and product system requirements for the Cisco Aironet 1100 Series.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 1 Key Features and Benefits

Feature	Benefit
Enterprise Performance	
2.4 GHz 802.11g or 802.11b radio, configurable up to 100 mW	• High-performance 2.4 GHz WLAN solution that delivers data rates of up to 11 Mbps (IEEE 802.11b) or 54 Mbps (IEEE 802.11g) with backwards compatibility to legacy 802.11b equipment • High-quality transmitter and receiver design provides long range and reliable coverage
Cisco IOS Software	• Provides end-to-end solution support for intelligent network services • Produces predictable and consistent network behavior • Delivers uniform applications and services
Virtual LAN (VLAN) support	• Allows segmentation of up to 16 user groups • Increases system flexibility, accommodating clients with different security requirements and capabilities
Quality of Service (QoS)	• Prioritizes traffic for different application requirements • Improves voice and video user experience
Proxy Mobile IP in Cisco IOS Software	• Provides seamless roaming between subnets • Enhances mobility of voice over 802.11 wireless
Wireless Domain Services (WDS)	• Component of Cisco SWAN • Collection of Cisco IOS Software features enhance WLAN client mobility and simplify WLAN deployment and management • Supports radio management aggregation, fast secure roaming and WAN link remote site survivability
Fast Secure Roaming	• Allows authenticated client devices to roam securely from one access point to another without any perceptible delay during reassociation • Supports latency-sensitive applications such as VoIP, ERP and Citrix
WAN Link Remote Site Survivability	• Allows the access point to act as a local RADIUS server to IEEE 802.1X authenticate wireless clients when the AAA server is not available • Provides remote site survivability and backup authentication services during WAN link or server failure
Client Address Resolution Protocol (ARP) Caching	• Allows Cisco Aironet access points to respond to Address Resolution Protocol (ARP) requests on behalf of IEEE 802.11 Cisco Aironet, Cisco Compatible Extensions and most Wi-Fi Certified wireless client devices • Enables IP address resolution without requiring the wireless client device to leave power save or idle modes • Extends client device battery life
RADIUS Server per SSID	• Allows specification of RADIUS servers on a per SSID basis by leveraging access point multiple SSID capabilities • Beneficial for multi-tenant deployments, such as airports, where each tenant desires a separate RADIUS server for user authentication

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 1 Key Features and Benefits

Feature	Benefit
Manageability	
Support for Cisco Discovery Protocol, SNMP standard MIB I and MIB II	• Interoperable with Simple Network Management Protocol (SNMP)-compliant network management systems such as HP OpenView and CA Unicenter • Manageable by many CiscoWorks applications in Resource Manager Essentials (Inventory Manager, Software Image Manager, Availability Manager), Campus Manager (Topology Services), and CiscoView
Cisco CLI supports Telnet, FTP, and TFTP	• Provides interface familiar to large community of network managers • Enables centralized management of remote access points • Facilitates standardization of network configuration
Support for Cisco SWAN	• Comprehensive Cisco framework for deploying, operating and managing hundreds to thousands of Cisco Aironet access points using the Cisco infrastructure • Extends to the wireless LAN the same level of security, scalability, and reliability that customers have come to expect in their wired LAN by introducing "wireless-aware" capabilities into the Cisco infrastructure • Includes CiscoWorks WLSE
Secure	
40-bit, 128-bit WEP	• Supports standards-based security methods for interoperability
Supports Cisco Wireless Security Suite	• Provides award-winning WLAN security features • Defends against passive and active security attacks • 802.1X and EAP-based authentication leverages user access lists • Supports RADIUS server for user login registry • Includes TKIP encryption enhancements • 802.11g version is AES ready with full support in 2004 • Supports Wi-Fi Protected Access (WPA), the new Wi-Fi Alliance specification for interoperable, standards-based wireless LAN security
Scalability	
Range of management and security options	• Autonomous management and security features scale with evolving architecture • Requires minimal initial investment
Configurable transmit power	• Facilitates cell-size management • Coverage can be decreased as deployment density requirements to optimize bandwidth increase
Availability	
Hot standby	• Fails over seamlessly to standby access point
Load balancing	• Distributes user connections across available access points • Optimizes aggregate throughput
Auto rate scaling	• Sustains connectivity at outlying distances
Investment Protection	
802.11g and 802.11b-compliant	• Support newer-high speed 802.11g clients as well as installed base of 802.11b clients • Mature technology incorporates generations of enhancements

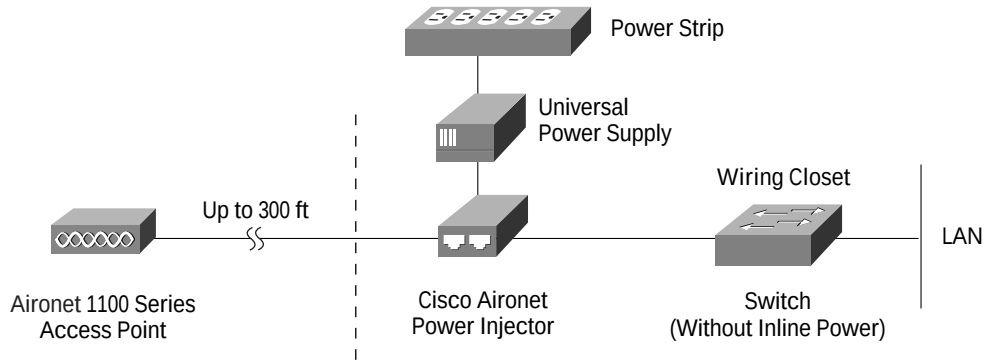
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 1 Key Features and Benefits

Feature	Benefit
Integrated Encryption Engine	• 802.11b version provides an integrated RC4 encryption engine for WEP, TKIP and WPA security • 802.11g version provides both an RC4 and AES encryption engine for WEP, TKIP, WPA and 802.11i support—hardware implementation maximizes performance • Firmware upgrade for AES support available 2004 (802.11g version only)
Storage that is more than twice the size of the initial firmware load	• Provides extra capacity for follow-on feature releases
Anti-theft security slot and security hasp	• Supports standard security cables or padlocks (not included) • Locks can be single- or master-keyed for simplified inventory management
Simplified Deployment	
Flexible mounting orientations	• Supports installation for a wide range of locations including walls, ceilings, desktops, and cubicle partitions
Integrated diversity dipole antennas	• Compact antenna profile • Spherical coverage pattern is optimized for any orientation • Diversity antennas improve reliability in high multipath environments such as offices
Auto-channel selection	• Determines and selects least congested channel
Supports Inline power over Ethernet (Figures 8, 9, 10)	• Eliminates need for local AC power • Reduces cable clutter • Enables deployment in remote locations
HTTP server with redesigned Web browser-based GUI	• Navigable graphic-oriented layout common across Cisco products • Express Set Up consolidates key configuration tasks in single view
Dynamic Host Configuration Protocol (DHCP) client	• Automatically obtains an IP address from DHCP server

Figure 8

The Cisco Aironet 1100 Series can be powered over Ethernet with the optional inline power injector.



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 9

The Cisco Aironet 1100 Series can use Cisco Catalyst powered switches for power over Ethernet. See Table 3 for specific details.

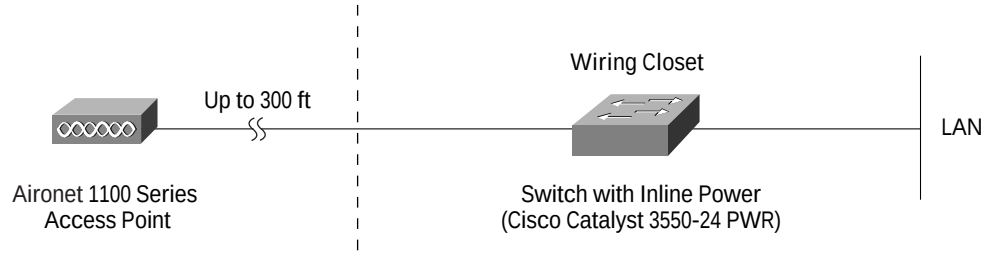


Figure 10

A Cisco Catalyst Inline Power Patch Panel can be used to power the Cisco Aironet 1100 Series over Ethernet.

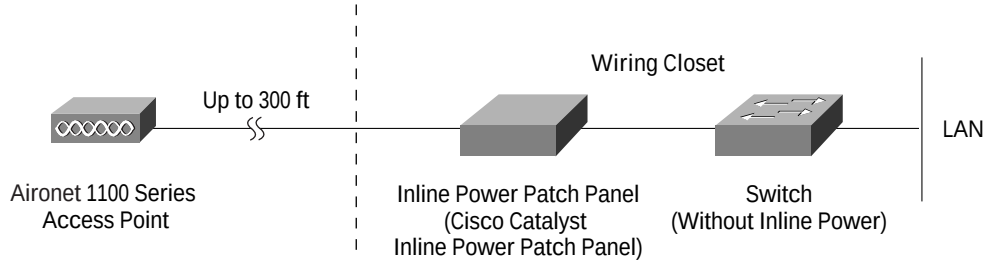


Table 2 Product Specifications

Item	Specification
Part number	• 802.11b: AIR-AP1120B-x-K9[1] • 802.11g: AIR-AP1121G-x-K9 • A=FCC • E=ETSI • I=Israel • J=TELEC (Japan) Customers are responsible for verifying approval for use in their country. Please see http://www.cisco.com/go/aironet/compliance to verify approval and to identify the regulatory domain that corresponds to a particular country. Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.
Data rates supported	• 802.11b: 1, 2, 5.5, 11 Mbps • 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
Network standard	• IEEE 802.11b or IEEE 802.11g
Uplink	• Autosensing 802.3 10/100BaseT Ethernet

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Product Specifications (Continued)

Item	Specification
Frequency band	• 802.11b: – 2.412 to 2.462 GHz (FCC) – 2.412 to 2.472 GHz (ETSI) – 2.412 to 2.484 GHz (TELEC) – 2.432 to 2.447 GHz (Israel) • 802.11g: – 2.412 to 2.462 GHz (FCC) – 2.412 to 2.472 GHz (ETSI) – 2.412 to 2.484 GHz CCK: (TELEC) – 2.412 to 2.472 GHz OFDM: (TELEC) – 2.432 to 2.447 GHz (Israel)
Network architecture type	• Infrastructure, star topology
Wireless medium	• 802.11g: Orthogonal Frequency Division Multiplexing (OFDM) • 802.11b and 802.11g: Direct sequence spread spectrum (DSSS)
Media access protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	• OFDM: – BPSK @ 6 and 9 Mbps – QPSK @ 12 and 18 Mbps – 16-QAM @ 24 and 36 Mbps – 64-QAM @ 48 and 54 Mbps • DSS: – DBPSK @ 1 Mbps – DQPSK @ 2 Mbps – CCK @ 5.5 and 11 Mbps
Operating channels	• 802.11b ETSI: 13; Israel: 4; Americas: 11; TELEC (Japan): 14 • 802.11g ETSI: 13; Israel: 4; Americas: 11; TELEC (Japan): CCK-14, OFDM-13
Nonoverlapping channels	• Three
Receive sensitivity	• 802.11b: – 1 Mbps: -94 dBm – 2 Mbps: -91 dBm – 5.5 Mbps: -89 dBm – 11 Mbps: -85 dBm • 802.11g: – 1 Mbps: -95 dBm – 2 Mbps: -91 dBm – 5.5 Mbps: -89 dBm – 6 Mbps: -90 dBm – 9 Mbps: -84 dBm – 11 Mbps: -88 dBm – 12 Mbps: -82 dBm – 18 Mbps: -80 dBm – 24 Mbps: -77 dBm – 36 Mbps: -73 dBm – 48 Mbps: -72 dBm – 54 Mbps: -72 dBm

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Product Specifications (Continued)

Item	Specification
Available transmit power settings	• 802.11b: CCK: – 100 mW (20 dBm) – 50 mW (17 dBm) – 30 mW (15 dBm) – 20 mW (13 dBm) – 5 mW (7 dBm) – 1 mW (0 dBm) • 802.11g: CCK: – 100 mW (20 dBm) – 50 mW (17 dBm) – 30 mW (15 dBm) – 20 mW (13 dBm) – 10 mW (10 dBm) – 5 mW (7 dBm) – 1 mW (0 dBm) OFDM: – 30 mW (15 dBm) – 20 mW (13 dBm) – 10 mW (10 dBm) – 5 mW (7 dBm) – 1 mW (0 dBm) • Maximum power setting will vary according to individual country regulations.
Range	**Indoor: Distance across open office environment** 802.11g (30 mW with 2.2 dBi gain diversity dipole antenna) • 90 ft (27 m) @ 54 Mbps • 95 ft (29 m) @ 48 Mbps • 100 ft (30 m) @ 36 Mbps • 140 ft (42 m) @ 24 Mbps • 180 ft (54 m) @ 18 Mbps • 210 ft (64 m) @ 12 Mbps • 250 ft (76 m) @ 9 Mbps • 300 ft (91 m) @ 6 Mbps 802.11b (100 mW with 2.2 dBi gain diversity dipole antenna) • 160 ft (48 m) @ 11 Mbps • 220 ft (67 m) @ 5.5 Mbps • 270 ft (82m) @ 2 Mbps • 410 ft (124 m) @ 1 Mbps **Outdoor:** 802.11g (30 mW with 2.2 dBi gain diversity dipole antenna) • 250 ft (76m) @ 54 Mbps • 600 ft (183 m) @ 18 Mbps • 1300 ft (396 m) @ 6 Mbps 802.11b (100 mW with 2.2 dBi gain diversity dipole antenna) • 1000 ft (304 m) @ 11 Mbps • 2000 ft (610 m) @ 1 Mbps Ranges and actual throughput vary based upon numerous environmental factors so individual performance may differ.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Product Specifications (Continued)

Item	Specification
Compliance	**Standards** • *Safety* – UL 1950 – CSA 22.2 No. 950-95 – IEC 60950 – EN 60950 • *Radio Approvals* – FCC Part 15.247 – RSS-210 (Canada) – EN 300.328 (Europe) – ARIB-STD 33 (Japan) – ARIB-STD 66 (Japan) – AS/NZS 3548 (Australia and New Zealand) • *EMI and Susceptibility (Class B)* – FCC Part 15.107 and 15.109 – ICES-003 (Canada) – VCCI (Japan) – EN 301.489-1 and -17 (Europe) – Security – 802.1X and TKIP – WPA – AES ready (802.11g version) • *Other* – IEEE 802.11b and IEEE 802.11g – FCC Bulletin OET-65C – RSS-102
SNMP compliance	• MIB I and MIB II
Antenna	• Integrated 2.2 dBi diversity dipole antennas
Security architecture client authentication and encryption	**Cisco Wireless Security Suite including:** • Authentication – 802.1X support including LEAP, PEAP, EAP-TLS, EAP-TTLS and EAP-SIM to yield mutual authentication and dynamic, per-user, per-session WEP keys – MAC address and by standard 802.11 authentication mechanisms • Encryption – Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits – TKIP encryption enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation via Cisco TKIP or WPA TKIP – AES ready with full support in 2004
Status LEDs	• Three indicators on the top panel report association status, operation, error/warning, firmware upgrade, and configuration, network/modem, and radio status
Software and device management and topology	• CiscoWorks CiscoView, Resource Manager Essentials, and Campus Manager
Remote Configuration Support	• BOOTP, DHCP, Telnet, HTTP, FTP, TFTP, and SNMP

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Product Specifications (Continued)

Item	Specification
Dimensions	• 4.1 in. (10.4 cm) wide; 8.1 in. (20.5 cm) high; 1.5 in. (3.8 cm) deep
Weight	• 10.5 oz. (297 g)
Environmental	• 32–104 F (0–40 C) • 10–90% humidity (noncondensing)
System Memory	• 16 MB RAM • 8 MB FLASH
Input Power Requirements	• 100–240 VAC 50–0Hz (power supply) • 33–57 VDC (device)
Power Draw	• 4.9 watts, RMS
Warranty	• One year
Wi-Fi Certification	

1. x=regulatory domain

Table 3 Product System Requirements

Feature	System requirement
Standard 802.1X-compliant user-level authentication and dynamic encryption keying	One of the following RADIUS servers: • Cisco Secure Access Control Server Version 3.0 or greater • Cisco Access Registrar® Version 3.0 or greater • Funk Software Steel Belted RADIUS Server Version 3.0 or greater • Interlink Networks RAD-Series RADIUS Server Version 5.1 or greater
CiscoWorks RME/Campus Manager	• CiscoWorks LAN Management Solution (LMS) or Routed WAN Solution (RWAN)
Line power over Ethernet support	• Cisco AIR-PWRINJ3= Aironet Power Injector for the 1100 and 1200Series • Cisco AIR-PWRINJ-FIB= Aironet Power Injector Media Converter • Cisco Catalyst® 3550-24 PWR Switch • Cisco Catalyst 4006 and 6500 Series switches with inline power • Cisco WS-PWR-PANEL Midspan Power Patch Panel

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Cisco SMARTnet Support and SMARTnet Onsite Support

Operational technical support service for maximizing network availability is offered through Cisco SMARTnet® support and SMARTnet Onsite support. Cisco SMARTnet support augments the resources of your operations staff; it provides them access to a wealth of expertise, both online and via telephone; the ability to refresh their system software at will; and a range of hardware advance-replacement options. Cisco SMARTnet Onsite support provides all SMARTnet services and complements the hardware advance-replacement feature by adding the services of a field engineer, critical for those locations where staffing is insufficient or unavailable to replace parts.

To learn more about service and support for the Cisco Aironet 1100 Series, visit:
http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/ps2978/serv_home.html

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see Cisco Technical Support Services or Cisco Advanced Services.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

203181_ETMG_JS_05.04